I.J. Information Engineering and Electronic Business, **2015, 6, 15-22**
Published Online November 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2015.06.03

Amplification-based Attack Models for Discontinuance of Conventional Network Transmissions

Mina Malekzadeh
Faculty of Electrical and Computer Engineering, Hakim Sabzevari University Sabzevar, Iran
Email: m.malekzadeh@hsu.ac.ir

Moghis Ashrostaghi
Engineering Faculty of Golestan University, Gorgan, Iran
Email: moghis.ashrostaghi@gmail.com

M.H. Shahrokh Abadi (IEEE Member)
Faculty of Electrical and Computer Engineering, Hakim Sabzevari University Sabzevar, Iran
Email: mhshahrokh@hsu.ac.ir

***Abstract*—**Amplification attacks take advantage of insecurity of different OSI layers. By targeting broadcast address of the victim networks and sending a few packets by the attackers, they force the legitimate user in the victim networks to response to these packets and attack their own trusted networks unknowingly. Despite importance of amplification attacks, there is not any work to implement these attacks to identify their procedure and quantify and compare their impacts on the networks. In this work, we use NS2 to achieve these goals. A variety range of scenarios are designed to implement DDoS amplification attacks and collect the results in terms of different network performance measures. The quantitative results prove devastating impact of the attacks which are easily capable of rendering the target wireless networks disable for their legitimate users.

***Index Terms*—**Amplification-based attacks, DDoS, Smurf attacks, Fraggle attacks NS2.

I. INTRODUCTION

An Amplification-based DDoS attack consists of an attacker, an amplification network and a victim host. An amplification network is essentially a network of host computers which permits broadcast messages. The amplification occurs because a single broadcast packet sent from the attacker can trigger a response packet from all the host computers in the target network. In this work we distinguish two types of amplification attack which are fraggle and smurf DDoS attacks.

Regardless of the type of current communication networks such as wifi, Ethernet, or different generation of mobile networks, they typically function based on different layers of the OSI models. Possible security breaches corresponding to each layer open the entire network vulnerable to different types of attacks. Among these layers, due to their importance role in delivery of the data, the network and transport layers are commonly targeted by the attackers to achieve their goals. The vulnerabilities exist in these layers will expose the communication networks to different types of attacks. The two common attacks that target these two layers are Fraggle and smurf attacks.

Fraggle and smurf attacks are alike in targeting the same layers of the OSI model. However, there are some key differences between them which vary their influences on the target networks performance.

To conduct the smurf attack, the attacker monitors the target network to identify its broadcast IP address along with the IP address of the victim's system. Then he creates a specific forgery ICMP echo request packet with the IP of the victim's system as the source address and the target network broadcast IP as the destination address. The attacker sends this forgery packet to the target network. Upon reception, since the destination address is broadcast IP, all the receivers in the target network must send ICMP echo replies to the source address which is the victim's system thus amplifying the attack traffic. Thereby, the legitimate systems unknowingly look like attackers and the victim's machine seems to be target of the attack by the legitimate systems in his own trusted network. This attack is very beneficial to the attackers because while they are able to stay unknown and hidden, they can send small traffics with even a slow link to cause a large amount of junk replies on the target network naturally by itself. Repeating the attack will drain the available bandwidth of the target network and eventually bring it down.

The way that may prevent the smurf attacks is configuring the network systems so that they are non-responsive to broadcast ICMP echo requests and simply ignore them. Thus to avoid this, instead of using ICMP echo requests, the attackers conduct fraggle attacks by exploiting UDP packets which cannot be non-responsive in networks because they are used in many demanding applications and protocols such as VoIP, DHCP, DNS, SNMP, RIP, Video conferencing. A fraggle attack occurs when an attacker sends UDP requests (port 7) resulting in a large quantity of junk replies and finally causes the target network to lose connectivity to the Internet [1, 2].

These attacks perform destructive intrusions to shut their target networks down achieving their malicious intentions. The attackers even are able to use low-bandwidth connection to kill high-bandwidth connections [9].

Unfortunately, despite importance of these attacks for disrupting conventional data transmissions, we could not find any research to clear out important information to A) determine possibility of performing these attacks, B) the steps that when taken to the extreme by the attacker, can lead to system failure, C) detect the target networks responses to the attacks, and D) quantify the amount of damage imposed to target networks in order to analyze the impact and severity of the attacks. Revealing this information will identify anatomy and the in-depth process of these attacks. This information as the first fundamental step are key success factor to demonstrate the practical procedure of the attacks which in turn assist developing more accurate prevention methods to protect the networks against these attacks.

This work is the first attempt to implement and measure impact of the smurf and fraggle attacks and compare their severity. We use NS2 simulation tool to perform two types of attacks: DDoS smurf attacks and DDoS fraggle attacks. The attacks are committed under different network scenarios to evaluate the behavior of the target networks against different intentions and capabilities of the attackers. The rest of this work is organized as follow.

Section 2 reviews the current related researches about fraggle and smurf attacks. In Section 3 we propose and design an attack model to implement the DDoS smurf attacks and DDoS fraggle attacks using NS2 simulation environment. We present, analyze, and compare the experimental results in Section 4. Finally, the work is concluded in Section 5.

II. Related works

The fraggle attack was listed in [3] under the category of network/transport-level attacks. The concept of the attack was explained but the attack was not evaluated in terms of being practical or the amount of damage it would cause to the networks. The IP broadcast based attacks including smurf and fraggle are explained in [4]. They proposed that disabling the IP broadcasting can prevent these types of attacks. The prevention model is implemented using GloMoSim simulator in terms of delivery ratio and number of collisions. Based on the results, they show that disabling IP Broadcast can mitigate the effect of flooding based DDoS attack with larger extent.

In [6] the author implemented the smurf attack in a testbed against Windows XP and Ubuntu 9 systems. Through some screenshots, transmission of forgery packets related to smurf attack was shown. However, the work did not quantify the impact of the attack in terms of any network performance metric to show the amount of damages caused by the attack. The authors of [7] provided a survey on taxonomy of DDoS attacks, including smurf and fraggle. A list of the attacks along with the date and name of companies that the attacks conducted against them were provided to emphasize feasibility and severity of the attacks. They mentioned that the fraggle attack generates even more bad traffic and can create even more damaging effects than just a Smurf attack. However, there is no implementation of the attacks to investigate and present this subject. In [8] they theoretically described the existing methods to perform smurf Attack. However, there is not practical implementation of the attack. There are also few papers that only mention the effectiveness of the attacks without going into the further details [10,11].

As the background works clearly show, despite importance of the DDoS fraggle and DDoS smurf attacks, only a few researches have been written to investigate them. However, the existing researches do not offer a design to implement these attacks and compare their severity on the networks. As a result, very little is known or understood about resilience of networks against these attacks. This need is taken into account as the main motivation and contribution of this work.

III. Simulation setup and data collection

In this section, we present the design considerations that we follow to achieve our goal and also the criteria we use to measure the effectiveness of the attacks. Our aim is to develop an attack model capable of implementing DDoS smurf and DDoS fraggle attacks to assess the performance of IEEE 802.11 WLAN under these attacks. Therefore, we use NS2 to design an infrastructure wireless network with seven wireless hosts (WH) associated with an access point. The WH1 is considered as the main victim in the target network. The

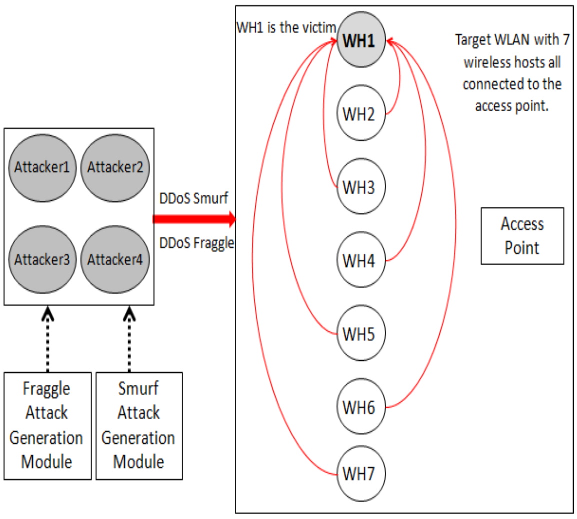

WH1 is the victim
WH1
WH2
WH3
WH4
WH5
WH6
WH7
Target WLAN with 7 wireless hosts all connected to the access point.
Access Point
Attacker1
Attacker2
Attacker3
Attacker4
DDoS Smurf
DDoS Fraggle
Fraggle Attack Generation Module
Smurf Attack Generation Module

Fig.1. Simulation topology

UDP with default size and interval in from of CBR packets are transmitted in the network. To measure the success rate of the attacks, three network metrics including throughput, delay, and packet lost ratio. These metrics determine the network behavioral pattern in both states; before being attacked and during the attacks. Fig. 1 shows the network topology and configuration we design to be used during the experiments.

A. Attack Planning: Scenarios and Settings

This section presents the implementation and experiments. In this work, the DDoS smurf and fraggle attacks are conducted with the primary intent of targeting WLAN. Considering main goal of this work, we design multiple security attacks scenarios that particularly change and test variety capabilities of the attackers and also internal conditions of the networks against the attacks. All the attack scenarios are individually tested and compared to analyze if the attack could compromise security and to what extent. The scenarios mainly focus on:

- Changing the number of attackers: the scenarios vary the number of attackers from one attacker (to simulate DoS fraggle and DoS smurf) to two and then four attackers (to illustrate and compare DDoS fraggle and DDoS smurf attacks).
- Changing the attack traffic parameters: the scenarios evaluate two different low-rate attack intervals (AI), 0.02s and 0.01s, to measure any variation affecting the progress of the attacks on the target WLAN. The reason of selecting such a low-rate attack is that generally the low-rate attacks are harder to detect because of their low average attack rate and various attack patterns.

By associating the above parameters with the three performance metrics, eighteen different attack scenarios along with the corresponding settings are summarized in Table 1 while the overall attack methodology is presented in Fig. 2.

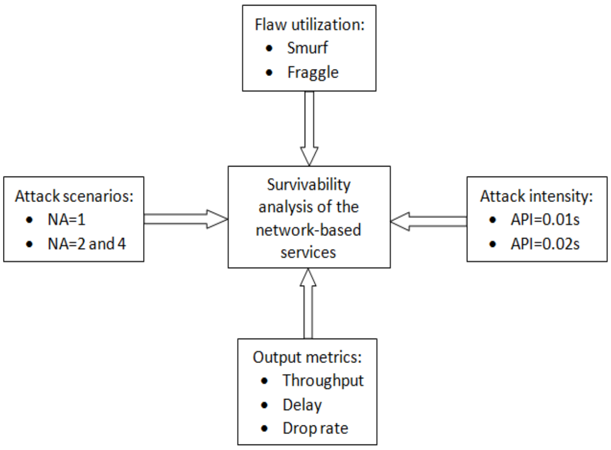


Fig.2. Attack methodology

Table 1. Scenario settings used in the experiments

Attack type	DDoS Fraggle, DDoS Smurf
Number of attackers (NA)	1, 2, 4
attack packets interval (API)	0.01s, 0.02s
Performance metrics	Throughput, Drop rate, Delay

B. Verification of the Attack Success Rate

The entire simulation time is 60 seconds which is divided into three parts: the first 20 seconds (0-20s) represents the behavioral pattern of the network before being attacked, the second 20 seconds (20-40s) shows the condition of the network under the attacks, and the last 20 seconds (40-60s) indicates status of the network after the attacks are over.

IV. Simulation Results

The attack scenarios that are developed in this work primarily provide a better simulation of realistic DDoS smurf and DDoS fraggle attacks. This section represents the experimental results from implementing the 18 scenarios which are collected and aggregated to assess the success rate and also compare severity of these attacks.

A. Experiments with NA=1

In this experiment we measure the performance variable of the target WLAN when launching the attack from a single source. In order to do this, a single attacker independently directs once smurf and then fraggle packets with 0.02s interval toward the target WLAN. The consequences of these attacks are compared in Fig. 3 in term of our performance metrics. The results show a high degradation in the network performance while it is still operational. The results clearly confirm higher success rate of the smurf attack in compare to the fraggle under the similar conditions. Based on the results, at the time when smurf attack was in progress, the number of packet drops and network delay increased more rapidly than the fraggle attack. Comparatively, the throughput results also verify higher degradation during smurf against our WLAN than fraggle attack.

In order to investigate the attack impact on network transmission pattern when the attack interval decreases, we repeated the above experiment but this time by setting the API to 0.01s. The results in terms of our performance metrics are presented in Fig. 4.

The performance measures quantitatively, like our previous experiment, prove more efficiency of smurf over fraggle attack. The direct impact of decreasing the API on degrading the network performance particularly on fraggle attack is also clearly concluded from the results. During the attack time (20-40s) the target network is hardly able to be functional for its legitimate WHs particularly when it is targeted by the smurf attack.

Based on these results it is concluded that an attacker with even a bandwidth much lower than the target network can highly disrupt the normal network transmission. Our very low attack rate while does not consume much of the attacker's bandwidth, it will hide the attack source and cause remarkable damage to the target WLAN.

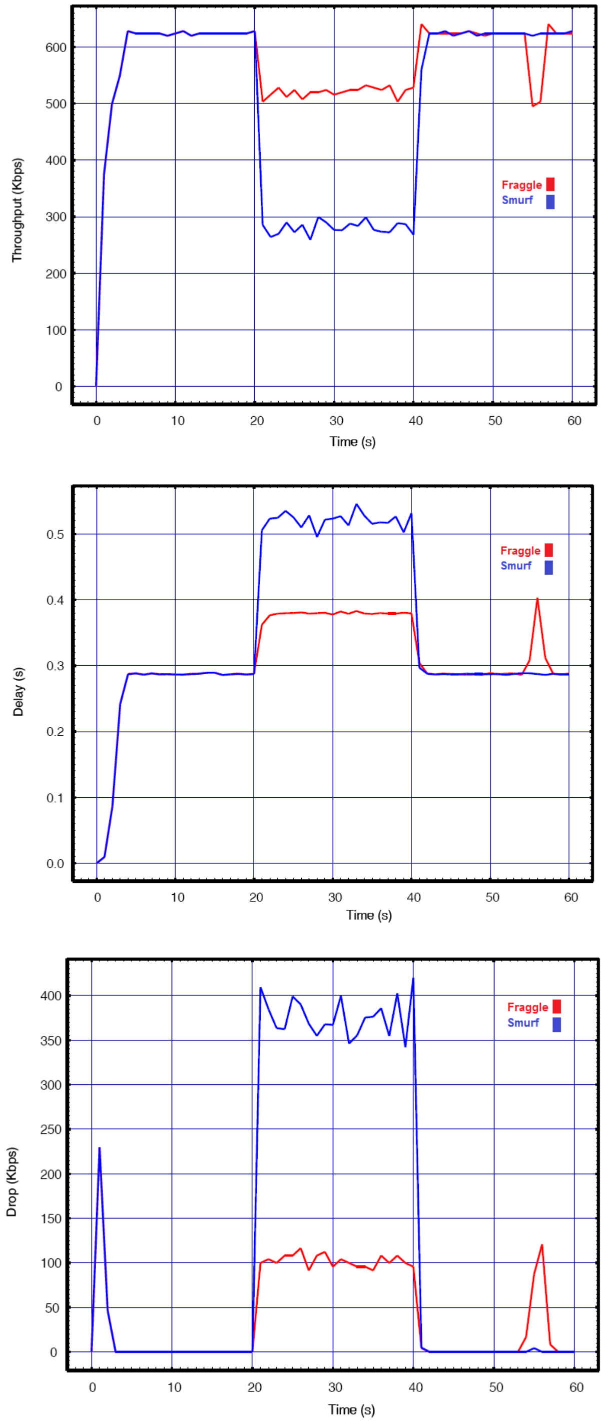


Fig.3. Smurf vs. Fraggle with API=0.02 for a) Throughput, b) Delay, c) Lost rate

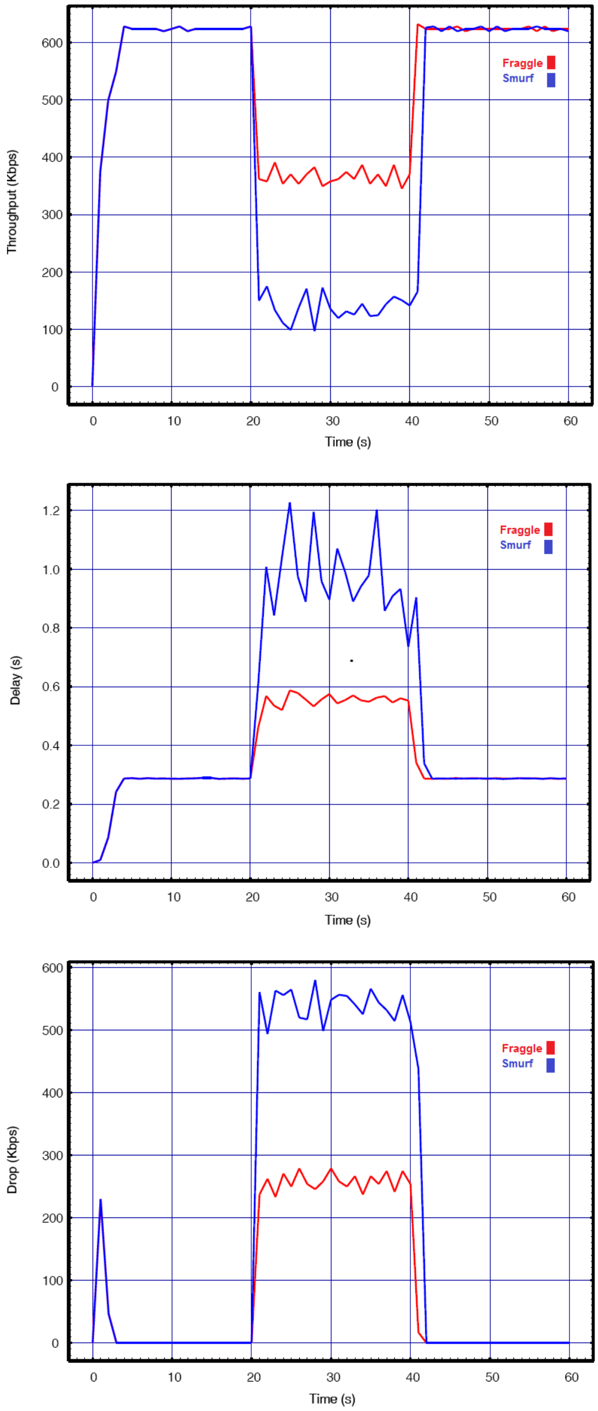


Fig.4. Smurf vs. Fraggle with API=0.01 for a) Throughput, b) Delay, c) Lost rate

B. Experiments with NA=2

The above experiments conduct and compare DoS smurf and DoS fraggle on the WLAN. In contrast, in this experiment we conduct and compare DDoS smurf and DDoS fraggle. The motivation is that generally implementing the attacks from multiple sources than a single source while results in increasing the effectiveness of the attack, makes it more difficult to identify the sources. Therefore, in this experiment the attacks are conducted against the WLAN by two attackers with API equal to 0.02s. The overall network performance under these DDoS attacks is presented in Fig. 5.

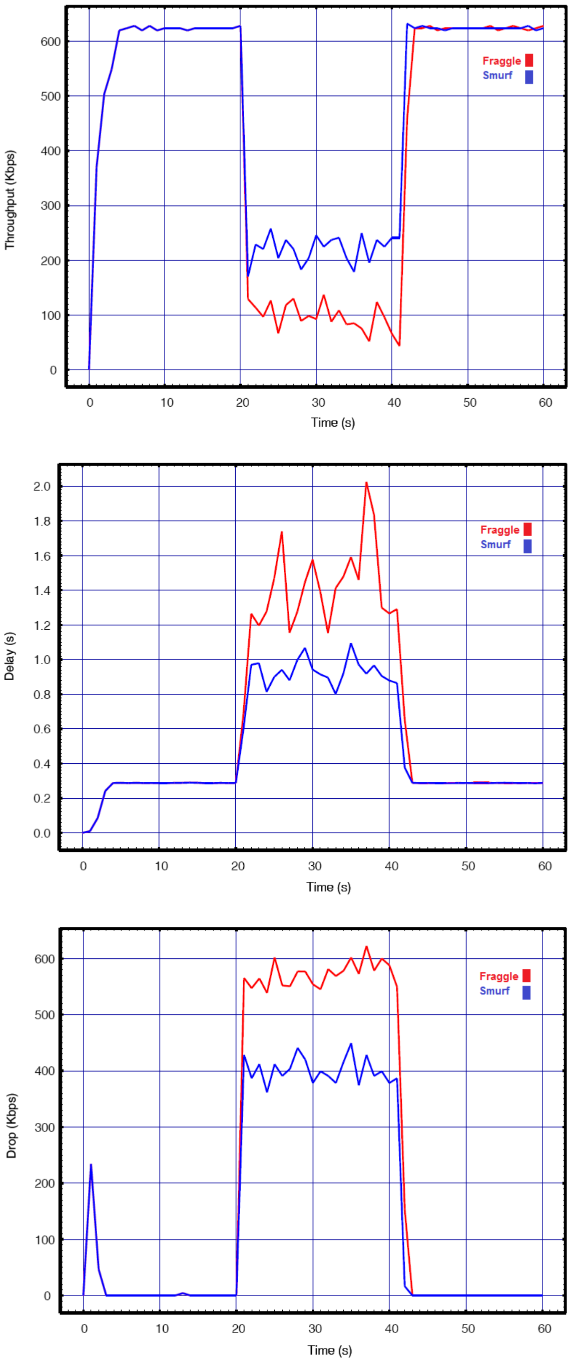


Fig.5. Smurf vs. Fraggle with API=0.02 for a) Throughput, b) Delay, c) Lost rate

Based on the results given above we can see that impact of the smurf and fraggle attack on the performance of WLAN targeted by two attack sources is remarkably more severe than one source. By increasing the number of attackers, the attacks create even more damaging effects than before and put tremendous pressure over the target WLAN. However, we can see that by increasing the number of attackers the results completely differ from our previous experiment with a single attacker. According to the results with one source of attack, regardless of the amount of API, the smurf attacks cause more damage to the target networks than the fraggle. However, when the network is being attacked by two attackers, the results show the DDoS fraggle is more effective and can degrade the network performance higher than the DDoS smurf. Since the above results show that the DDoS smurf has more destructive effects on the target network than the DDoS fraggle, we decided to examine the impact of these DDoS attack by decreasing the API. Thus, like before, we changed the API to 0.01s and repeated the experiment. The results are presented in Fig. 6.

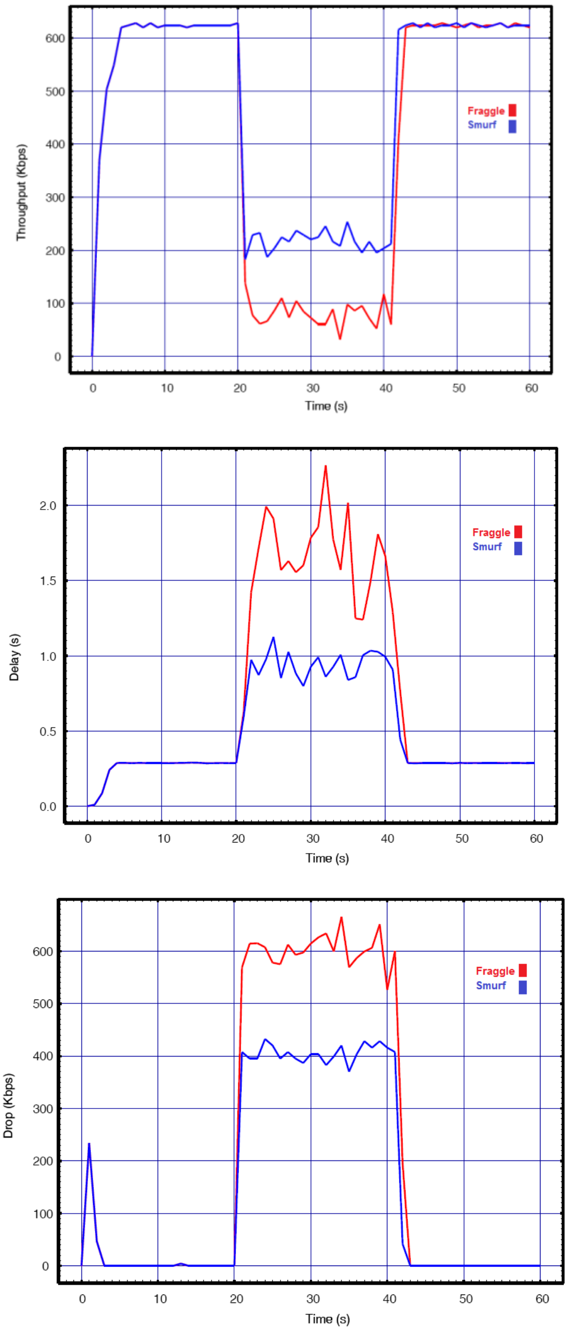
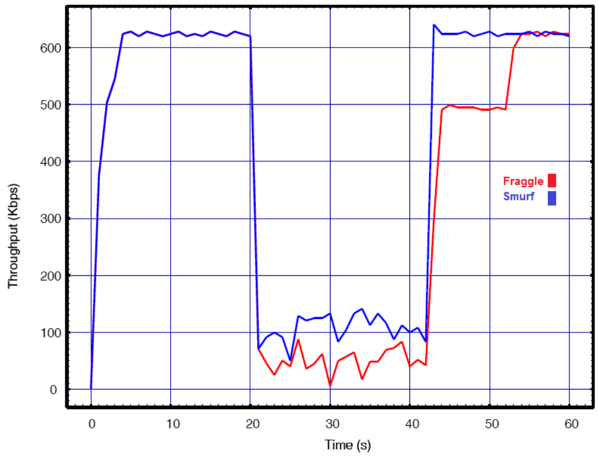


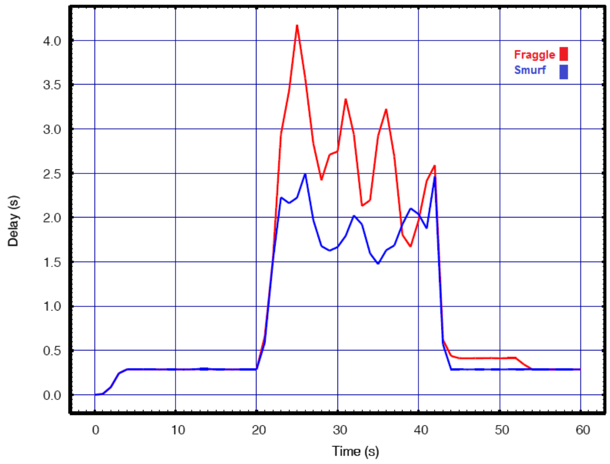
Fig.6. Smurf vs. Fraggle with API=0.01 for a) Throughput, b) Delay, c) Lost rate

The obtained results also confirm the previous difference when comparing to the results of the single source attacks. We can see form the above results that by with two attack sources, the fraggle is more destruction than the smurf attacks even when decreasing the API to 0.01s. We also see from the results that when we decreased the API to 0.01s in single source attack, the performance was highly degraded. For example the throughput results of single attack source decreased from 600 to 300 and to 150 during smurf attack with API=0.02s and API=0.01s respectively. However, as we implement the DDoS by increasing the NA to two attackers, the difference between the impact of the 0.02s API and 0.01s API on network performance is small. For example the throughput results of two attack sources decreased from 600 to 250 and to 220 during smurf attack with API=0.02s and API=0.01s respectively. The reason is related to huge number of amplification traffics and the corresponding collisions. According to the results, the WLAN is practically unable to perform its normal functions while the huge increase in the amount of delay and lost packets prove the extensive corruption of normal communications.

C. *Experiments with NA=4*

From the above experiments and their corresponding results, we observed that when performing DoS attack, the smurf is more effective than DoS fraggle on network performance degradation. However, when conduction DDoS attacks, the fraggle is more destructive than smurf. Therefore, in order to reach to a conclusion we increase the number of attackers to again perform DDoS fraggle and DDoS but this time with four attackers. The goal is to investigate the correlation between the number of attackers on possible impact of the DDoS fraggle and DDoS smurf on wireless networks. The results are presented in Fig. 7.





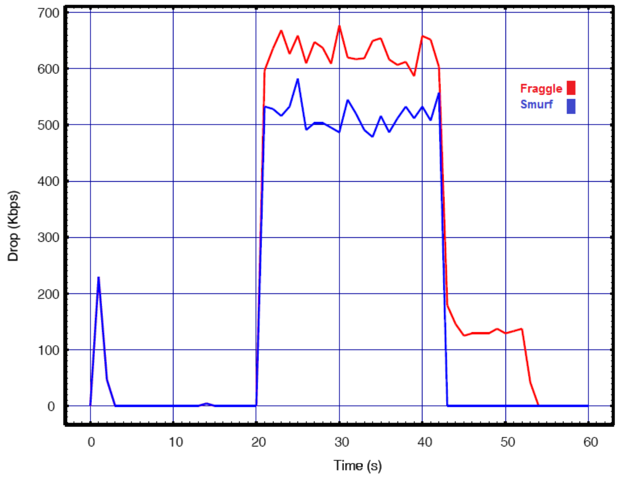


Fig.7. Smurf vs. Fraggle with API=0.02 for a) Throughput, b) Delay, c) Lost rate

The above results show that even a very low rate DDoS smurf or DDoS fraggle can bring the wireless network to a complete halt. In this experiment we increase the number of attackers to four and according to result even 0.02s API can disable the network functionality. During either the attacks throughput drops to closely to zero while none of the legitimate packets were able to reach to destination and they all dropped during the attack. The results of both attacks in this experiment are closer than the others which show high effectiveness of them on corrupting the transmissions of the legitimate wireless hosts. In order to examine and compare impact of the attacks by decreasing the attack interval, we repeated this experiment with 0.01s as our API. The results are presented in Fig. 8.

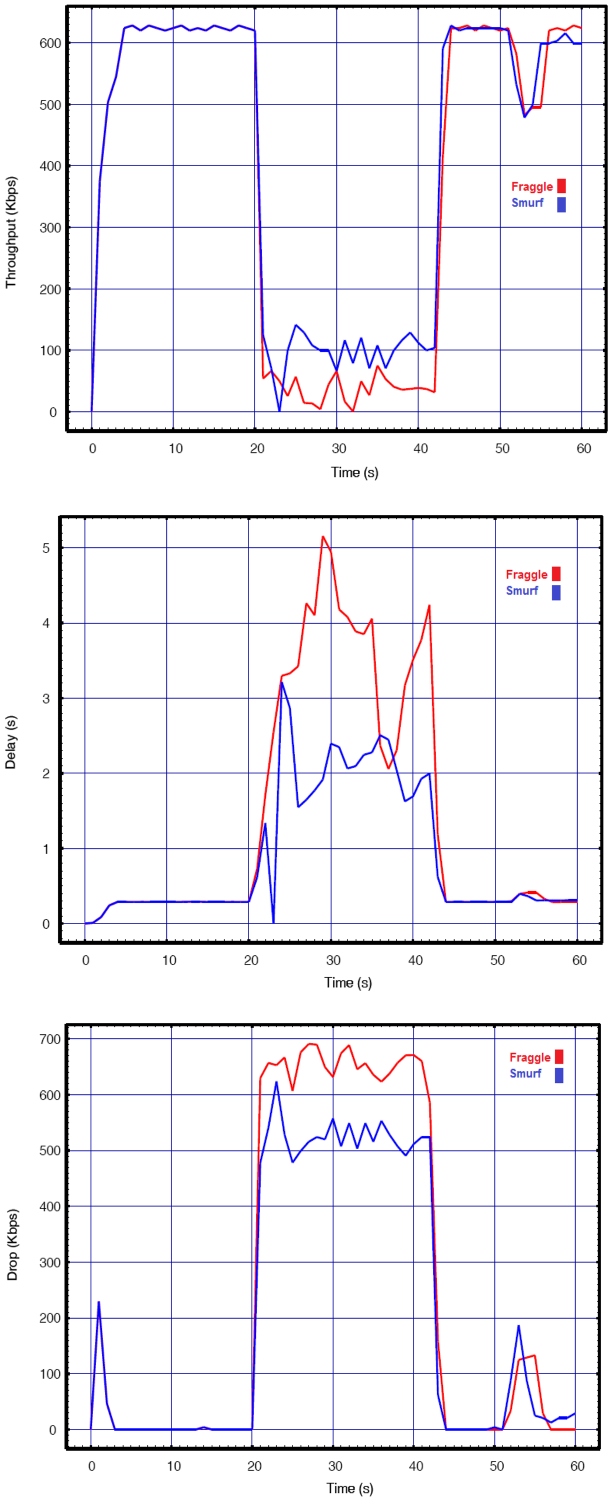


Fig.8. Smurf vs. Fraggle with API=0.01 for a) Throughput, b) Delay, c) Lost rate

From the above experimental results the devastating impact of the attacks is observed. During the entire attack time, the bandwidth was overwhelmed by the huge number of the legal packets of WHs in response to the fewer number of packets sent from the four attackers.

V. Conclusion

In this work we design different scenarios in order to implement and compare the effectiveness of the low rate fraggle and smurf attacks in terms of DoS and DDoS attacks on performance of IEEE 802.11 wireless networks. According to the results both attacks are highly capable of disabling the target network for its legitimate users even when the attackers use a limited bandwidth. By the above experimental results, we reach a conclusion that the smurf attacks are more destructive than fraggle attacks when the target network is attacked by DoS. The results show that DoS smurf can degrade wireless network higher than DoS fraggle in terms of the performance measures. However, if the attackers are able to distribute their ability and launch the attacks from different sources, the DDoS fraggle attacks cause more damage to the network than DDoS smurf.

References

[1] V. BOCAN. Developments in DoS Research and Mitigating Technologies, Transactions on Automatic Control And Computer Science, 2004, Vol.49, No.63, PP.1-6.

[2] C. Douligeris and A.Mitrokotsa. DDoS attacks and defense mechanisms: classification and state-of-the-art, 2004, Elsevier Computer Networks, PP. 643–666.

[3] S.T.Zargar, J.Joshi, D.Tipper. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, 2013, IEEE Communications Surveys & Tutorials, PP.1-24.

[4] M.Kumar and N.Kumar. Detection and prevention of ddos attack in manet’s using disable ip broadcast technique, 2013, International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol.2, No.7, PP.29-36.

[5] A.Vince Paual , P. Anuranj, K. Prasadh. Enhanced Attack Resistance Scheme for App-DDoS Attacks using Bayes Optimal Filter Strategy, International Journal of Computer Applications, 2012, PP.14-18.

[6] H.C. Chaudhari and L.U. Kadam. Wireless Sensor Networks: Security, Attacks and Challenges, International journal of networking, Vol.1, No.1, pp.4-16, 2011.

[7] C.M. Pate and V.H. Borisagar. Survey On Taxonomy Of DDoS Attacks With Impact And Mitigation Techniques, International Journal of Engineering Research & Technology (IJERT), Vol.1, No.9, pp.1-8, 2012.

[8] K. Choudhary, Meenakshi, and Shilpa. Smurf Attacks: Attacks using ICMP, International Journal of Computer Science and Technology (IJCST), Vol.2, No.1, pp.75-77, 2011.

[9] N.Ahmed, Z.I.A.Khalib, R.B.Ahmad, S.Sudin, S.Asi, Y.Laalaoui. Low-End Embedded Linux Platform for Network Security Application – Smurf Based Attack Detection, 2008, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.11, PP.1-7.

[10] D.Kale and V.Bhosale. Scrutiny of DDoS Attacks Defense Mechanisms, International Journal of Advanced Research in Computer Science & Technology, 2014, Vol.2, No.1, PP.154-157.

[11] D.G.Kumar, C. V. Guru Rao, A.Gopal J, and P.Mohan. Distributed DoS Attacks: Classification and Defense Mechanisms, 2013, PP.703-708.

Authors' Profiles

Mina Malekzadeh is an assistant professor and lecturer in the department of computer science at Hakim Sabzevari University. Her research interests include communication networks, network security, VoIP, and system development programming. She holds a Doctoral degree in computer security from UPM, MSc in software engineering from UPM, BSc in Computer Science from SBU.

Moghis Ashrostaghi received the B.S. degree in Computer Science from Golestan University. He is currently a master student. His research interests are Computer Networks and wireless security.

M.H Shahrokh Abadi is an assistant professor and lecturer in the electrical and computer engineering faculty at Hakim Sabzevari University. He received his Ph.D. and Master from the University of Putra Malaysia. His research interests are thick film and sensors.

How to cite this paper: Mina Malekzadeh, Moghis Ashrostaghi, M.H. Shahrokh Abadi,"Amplification-based Attack Models for Discontinuance of Conventional Network Transmissions", IJIEEB, vol.7, no.6, pp.15-22, 2015. DOI: 10.5815/ijieeb.2015.06.03